

CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

- 1 1. A hardware implementation of a crypto-function comprising:
 - 2 a first register storing data to be encrypted or decrypted;
 - 3 a second register for receiving data which has been encrypted or decrypted; and
 - 4 combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.
- 1 2. The hardware implementation of a crypto-function recited in claim 1, wherein the crypto-function is a block cipher algorithm.
- 1 3. The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the Data Encryption Standard (DES) algorithm.
- 1 4. The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the CHAIN algorithm.
- 1 5. The hardware implementation of a crypto-function recited in claim 2, wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times.
- 1 6. The hardware implementation of a crypto-function recited in claim 5, wherein the combination logic performs mixing, permutation and key-

3 dependent substitution in each round.

1 7. The hardware implementation of a crypto-function recited in claim 5,
2 wherein the combinational logic enciphers a block by performing an initial
3 permutation of a block to be enciphered and then a complex key-dependent
4 computation followed by a permutation which is an inverse of the initial
5 permutation.

1 8. The hardware implementation of a crypto-function recited in claim 7,
2 wherein the combinational logic deciphers a block by performing deciphering
3 using the same key as used to encipher the block in a process that is an inverse
4 of the enciphering process.

PCT/EP2019/000209